ENCRYPTION APPARATUS AND METHOD FOR SYNCHRONIZING MULTIPLE ENCRYPTION KEY WITH DATA STREAM

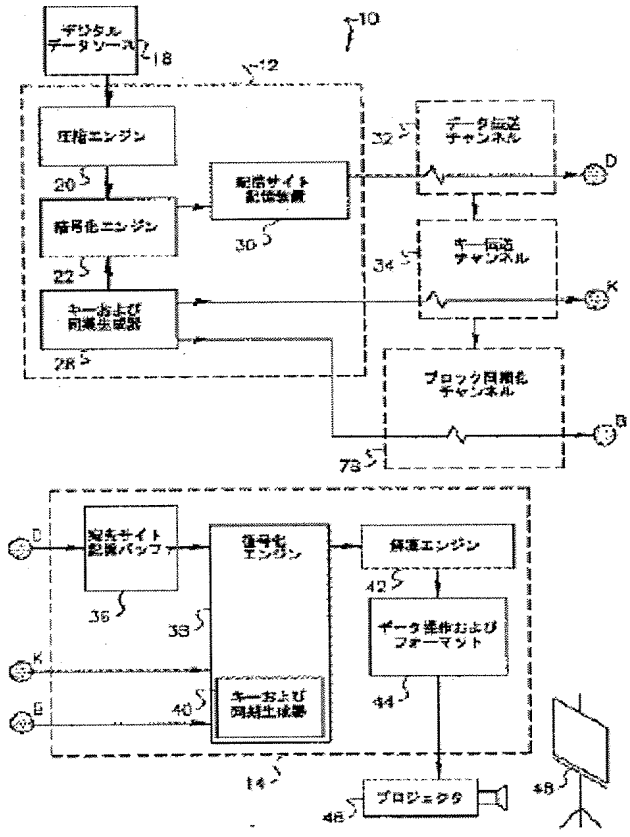
Publication number: JP2002141898
Publication date: 2002-05-17
Inventor: TEHRANCHI BABAK
Applicant: EASTMAN KODAK CO
Classification:
- international: ***G06F12/14; G06F21/24; H04L9/08; H04L9/12; H04N7/167;*** **G06F12/14; G06F21/00; H04L9/08; H04L9/12; H04N7/167;** (IPC1-7): H04L9/12; G06F12/14; H04L9/08
- European: H04N7/167D
Application number: JP20010272117 20010907
Priority number(s): US20000656634 20000907

Also published as:
EP1187483 (A2)
US7242772 (B1)
EP1187483 (A3)
CA2354351 (A1)

Report a data error here

Abstract of **JP2002141898**

PROBLEM TO BE SOLVED: To provide an apparatus and a method for encrypting a data stream as successive two or more data blocks to each of which an encryption key is assigned. SOLUTION: The data stream such as a digital moving picture is encrypted in units of one or more blocks, each block having the assigned encryption key. A plurality of encryption key is assigned to the complete stream. A synchronization index is provided for mapping each individual encryption key to its starting data block. The encryption keys and the related synchronization indices re provided separately from the data stream through the user of one or more additional data transfer mechanisms. A randomly generated optional offset changes an interval between the data blocks at which encryption is performed by a specified encryption key.



(19)日本国特許庁（ＪＰ）　(12) **公開特許公報**（Ａ）　(11)特許出願公開番号
特開2002－141898
（P2002－141898A）
(43)公開日　平成14年５月17日(2002.5.17)

(51)Int.Cl.[7]	識別記号	ＦＩ		テーマコード（参考）
Ｈ０４Ｌ　9/12		Ｃ０６Ｆ　12/14	３２０Ｂ	５Ｂ０１７
Ｇ０６Ｆ　12/14	３２０	Ｈ０４Ｌ　9/00	６３１	５Ｊ１０４
Ｈ０４Ｌ　9/08			６０１Ｚ	

審査請求　未請求　請求項の数５　ＯＬ　（全 16 頁）

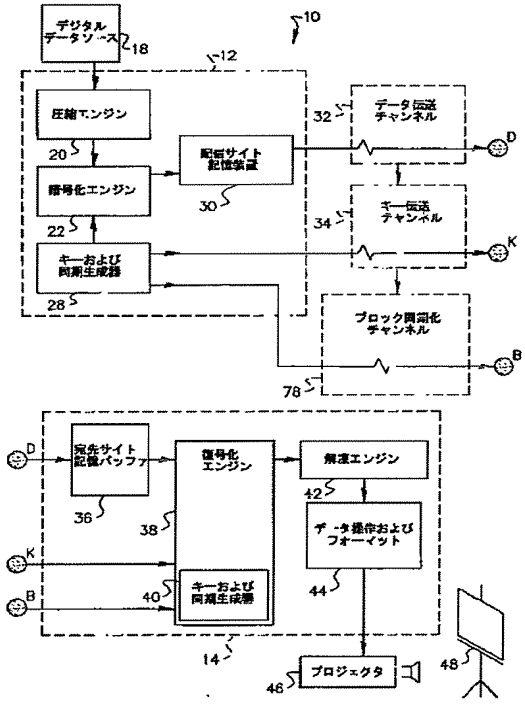
(21)出願番号　特願2001－272117(P2001－272117)
(22)出願日　平成13年９月７日(2001.9.7)
(31)優先権主張番号　０９／６５６６３４
(32)優先日　平成12年９月７日(2000.9.7)
(33)優先権主張国　米国（ＵＳ）

(71)出願人　590000846
イーストマン　コダック　カンパニー
アメリカ合衆国，ニューヨーク14650，ロチェスター，ステイト　ストリート343
(72)発明者　パパク・テーランチ
アメリカ合衆国14626ニューヨーク州ロチェスター、ホークス・ネスト・サークル341番
(74)代理人　100062144
弁理士　青山　葆　（外２名）

Ｆターム(参考)　5B017 AA06 AA07 BA07 CA15
5J104 AA03 AA16 EA22 NA02

(54)【発明の名称】　多重暗号化キーをデータストリームに同期させる暗号化装置および方法

(57)【要約】
【課題】　データストリームを、各々に暗号化キーが割り当てられた複数の順次データブロックとして暗号化する装置と方法とを提供する。
【解決手段】　本発明において、デジタル動画のようなデータストリームは、各々に暗号化キーが割り当てられた１以上のブロックのユニットで暗号化される。データストリームを完成するために複数の暗号化キーが割り当てられる。個々の暗号化キーをその先頭データブロックにマップする同期化索引が提供される。暗号化キーと関連する同期化索引とは、１以上の追加のデータ転送機構を利用して、データストリームとは別個に提供される。無作為に生成された随意的なオフセットは、特定の暗号化キーによって暗号化が実行されるデータブロック間の間隔を変化させることができる。



【特許請求の範囲】
【請求項１】　複数のデータブロックを、デジタルデータソースからデジタルデータ受信機まで、安全に転送するデータ転送装置であって、（ａ）前記複数のデータブロックの各々の単一データブロックに割り当てられる暗号化キー、および、前記暗号化キーと前記単一データブロックとの間の対応を示すブロック同期化索引を提供する暗号化キー生成器と、（ｂ）前記各々の単一データブロックに対して、前記暗号化キー生成器からの前記暗号化キーを用いて、暗号化されたデータブロックを生成する暗号化エンジンと、（ｃ）前記暗号化されたデータブロックを、前記暗号化エンジンから前記デジタルデータ受信機へ配信するデータ伝送チャンネルと、（ｄ）前記暗号化キーを、前記暗号化キー生成器から前記デジタルデータ受信機へ配信するキー伝送チャンネルと、（ｅ）前記ブロック同期化索引を、前記暗号化キー生成器から前記デジタルデータ受信機へ配信するブロック同期化データチャンネルとからなる装置。
【請求項２】　データストリームを、デジタルデータソースからデジタルデータ受信機へ、安全に転送する方法であって、（ａ）前記データストリームを、平均サイズと無作為に生成されたオフセットとに基づいて、各々のサイズが可変である複数の連続したデータブロックに分割するステップと、（ｂ）各々の連続するデータブロックに対して、暗号化キーを生成するステップと、（ｃ）前記各々の連続するデータブロックを、前記暗号化キーを用いて暗号化し、暗号化されたデータブロックを提供するステップと、（ｄ）前記暗号化されたデータブロックを前記暗号化キーに関連付ける同期化索引を生成するステップとからなる方法。
【請求項３】　デジタル動画像データストリームを、デジタルデータソースからデジタルデータ受信機まで、安全に転送する方法であって、（ａ）前記デジタル動画像データストリームを、複数のデジタル動画像データブロックに分割するステップと、（ｂ）複数の暗号化キーを生成するステップと、（ｃ）前記複数のデジタル動画像データブロックの各々に対して、
（１）前記各々のデジタル動画像データブロックを、識別可能な暗号化キーを用いて暗号化し、暗号化されたビデオデータブロックを生成するステップと、
（２）前記暗号化されたデータブロックを、前記暗号化されたデジタル動画像データストリームの一部として記憶するステップとからなるステップを繰り返すことにより、暗号化されたデジタル動画像データストリームを生成するステップと、（ｄ）前記各々のデジタル動画像データブロックを、前記各々の識別可能な暗号化キーと関連付ける同期化索引を生成するステップと、（ｅ）前記暗号化されたデジタル動画像データストリームを、前記デジタルデータ受信機に提供するステップと、（ｆ）前記同期化索引を、前記デジタルデータ受信機に提供するステップとから成る方法。
【請求項４】　複数の暗号化キーを、対応する複数の暗号化されたデータブロックにマッピングする方法であって、（ａ）前記複数の暗号化キーを、前記暗号化されたデータブロックとは別個に提供するステップと、（ｂ）マッピングアルゴリズムを前記複数の暗号化キーに相関させる識別子を提供するステップとからなる方法。
【請求項５】　動画の暗号化されたデジタル動画像データブロックを復号化する方法であって、
デジタル動画像データフレームまたはデジタル動画像データフレーム成分の識別を提供するステップと、
複数の暗号化キーから対応するキーを生成し、それを、前記デジタル動画像データフレームまたはデジタル動画像データフレーム成分がその一部を形成するデジタル動画像データブロックの復号化に使用するステップとからなる方法。
【発明の詳細な説明】
【０００１】
【発明の属する技術分野】本発明は、データストリームを、各々に暗号化キーが割り当てられた複数の順次データブロックとして暗号化および復号化する装置と方法に関し、より詳細には、各々の暗号化キーを、対応するデータブロックに確実に同期させる装置と方法に関する。
【０００２】
【従来の技術】例えば、大容量の携帯記憶装置や高速データ伝送チャンネルによって提供されるような、データストリームの伝送または転送に対する用途の拡張を利用するために、大量データ転送能力を必要とするユーザーは、高い安全性が提供されることを要求する。そのような安全対策により、データ改ざん、盗聴およびデータ著作権侵害などの行為を防止することができる。
【０００３】データ著作権侵害は、特に、ＴＶやビデオ番組のプロバイダー、および、デジタル映画のプロバイダーといった、データストリームとして伝送されるエンターテインメントのプロバイダーにとって脅威である。厳しい安全対策が行われなければ、例えば著作権で保護される作品のデジタルコンテンツが不法にコピーおよび頒布され、その結果、権利保有者の莫大な投資金の損失が発生するであろう。デジタル映画産業が発展するにつれ、データセキュリティの必要性はより重大になっている。映画がデジタル式に製作および配給されると、フィルムのコピーを地方の劇場へ配給するような従来の方法は変化すると思われる。衛星若しくはケーブルによる伝送を利用した配給、専用電話回線の経由による伝送を利用した配給、または、ＤＶＤ装置などの携帯式大容量記憶媒体を利用した配給のいずれにしても、現在のフィルムベースの配給は、映画作品のデジタル化に取って代わられる傾向にある。この発展は、エンターテインメント産業に対して、相当な潜在性リスクを提示する。それは、容認されたサイトのみがエンターテイメントの作品

にアクセスできるような安全対策によって対処されなければならない。

【０００４】動画像のデジタル化は、データセキュリティの確保にとって特に克服困難な課題を抱えている。このセキュリティ課題の一つは、ファイルのサイズである。デジタル化された省略されない形態のフィルムは、圧縮前に、２～３テラバイトオーダーのデータでありうる。そのため、最新のデータ圧縮技術をもってしても、標準的な映画が有するデータ量は相当なものである。このデータ容量と、復号すなわち解読された映画のコピーをアクセス可能な状態にする場合のリスクとにより、映画を映写すなわち表示するためのデジタルデータストリームの高速復号化を提供する（また、データ解凍の時間も与える）、高速またはリアルタイム復号化技術があれば、大変有益である。

【０００５】最善のセキュリティを確保する理想的な解決法は、ビデオデータ、動画像データ、動画データ（ここではデジタル動画像データとも表記し、デジタル映画および動画の意味にも使う。その放映媒体はテレビ、動画劇場、コンピュータのいずれでもよい。）を、フィルム編集や製作工程さえ含む全ての状況下で暗号化することである。この方法を用いれば、動画がどこで操作されようと、どこへ伝送されようと、最初の撮影段階から編集段階、最終的に映画館で放映されるまで、その動画のデジタルデータは、平文（暗号化されていない）形式でアクセス可能になることはない。しかし、同時に、編集等のために、１以上の個々のフレームにアクセスを許可する任意の暗号化方式が必要になる。

【０００６】セキュリティ課題の重要な点は、動画を、デジタルデータストリームとして、同時に何千ものサイトに配信する必要があるということである。これは、データの暗号化／複号化、圧縮／解凍、配信全般に対する解決法が頑強でなければならないことを意味する。また、これらの解決法は、多くの劇場で採用されている「時間差上映スケジュール」にも対応でき、再生や一時停止を必要としうる機器のトラブルのような難題を処理できなければならないので、やはり、復号化方式における個別フレームのアドレス表示や再同期化が必要である。ここで使用する暗号化という言葉は、その意味を隠すためのデータ変換を含んでおり、従って、圧縮や、画像の色彩、サイズおよび濃度に作用するように用いられる画像処理のような周知の暗号化とは区別される。

【０００７】ビデオやデジタル動画のフィルムのサイズを考慮すると、従来の暗号化処理では、暗号化セキュリティを維持する一方で、同時に、個々のフレームを許可するという難しい課題にうまく対処できない。例えば、デジタル動画を１ブロックとして暗号化する簡単な処理は、個々のフレーム編集、早送り、時差表示などの操作や、関連するフレームベース動作のサポートを困難にし、または、実行できなくする。従って、そのデータを複数のブロックに構文解析する処理は意味がある。しかし、この方法でも、各々のブロックに同じ暗号化キーを割り当てるなら、システムの安全性は十分ではない。そのため、データセキュリティを提供しつつ、個別ブロックにおいてデータを暗号化する柔軟な解決法が必要とされていることが認識される。

【０００８】基本的に、暗号化アルゴリズム自体が、個別ブロックにおける平文データ（すなわち、暗号化されて暗号テキストデータを形成する予定のデータ）の処理を必要とすることに着目してほしい。例えば、ＤＥＳ暗号化は、６４ビットのデータユニットで一度に作動する。暗号化方法は、暗号化する度に同じキーを再利用してもよいし、または、異なるデータブロックに異なるキーを使用してもよい。後で述べるように多重キーを使用すると、データを更に安全に暗号化できるという利点がある。

【０００９】例として、一般的な２つのタイプの暗号化方式がある。

（１）秘密または対称暗号化

対称アルゴリズムは、暗号化および復号化に同じキーを使用する。秘密キーを所有していれば誰でもデータを復号化できる。米国特許第３９６２５３９号（Ｅｈｒｓａｍ等による）において開示されるように、米国規格基準局の標準データ暗号化規格（ＤＥＳ）が、対称暗号化方式の例として周知である。

（２）公開または非対称暗号化

非対称アルゴリズムは、暗号化および復号化に異なるキーを使用する。データは、誰でもアクセス可能な公開キーを使用して暗号化される。しかし、データの復号化は、秘密キーを所有する者だけが行える。米国特許第４４０５８２９号（Ｒｉｖｅｓｔ等による）において開示されるＲＳＡと、米国特許第４２００７７０号（Ｈｅｌｌｍａｎ等による）において開示されるＤｉｆｆｉｅ－Ｈｅｌｌｍａｎの２つが、公開キー暗号化方式として周知である。

【００１０】一般的に、対称暗号化は、非対称暗号化よりも速く、従って、動画の暗号化や、同様のデータストリームの暗号化／複号化に採用されやすい。しかし、対称暗号化には、対称キーが、所望の各々の受信者に安全に配信される必要があるという欠点がある。他の受信者に対する不本意なアクセスを許可するというリスクを最小限に抑えなくてはならない。

【００１１】容量の大きいファイルの復号化に使用されるキーの配信と管理に対する従来の解決法は多数ある。例えば、この目的のために、対称と非対称の両アルゴリズムの長所を使用することが知られている。それには、まず、非対称暗号化を用いて１以上の対称キーを配信し、その後、これらのキーを使って短時間で復号化する。キーは暗号化されたデータを復号化するために必要とされる一連のビットまたは番号である。

【００１２】かなり大容量のデータストリームを効率的に復号化する従来の解決法の１つは、多重キーを提供することである。この方法において、キーは、データストリーム中の識別される複数ブロックにマップされる。ストリームの暗号化に使用されるキー管理処理の一例として、米国特許第６０５２４６６号（Ｗｒｉｇｈｔによる）は、公開キー暗号化方式の代わりに、暗号化に多重秘密キーを使用する方法を開示する。公開キー方式を使用して転送された初期キー生成情報に基づき、一連の等しい秘密キーが、送信サイトと受信サイトの両方で生成される。キーをそのデータストリームに同期化するために、生成された一連のキーの各々が、データストリーム内のページ上のあらかじめ決められた固定位置に索引付けられる。それ故、万一データパケットが損失した場合には、再同期化が行われる。ライト（Ｗｒｉｇｈｔ）の特許において使用されるキーからページへの直接マッピング方式は、パケット損失や再同期化による課題を軽減させる利点を有しているが、キーの再配列またはページ境界の操作を要求することによって任意の安全対策を提供するという試みは開示されていない。また、ライトの特許において開示される方法は、例えばデジタル動画に必要とされる安全なデータ転送に対して、別の固有の欠点も備える。例えば、キーを使用するための索引情報が、個別に提供されずに、暗号テキストメッセージ自体において暗号化される。さらに、同一の通信チャンネルが、キー交換と暗号テキストデータ伝送に使用される。この同一チャンネルの使用は、その通信チャンネルにアクセスできる者は誰でも、暗号化されたデータや復号化に必要な情報にアクセスできることを意味する。

【００１３】同様に、無線通信チャンネルについて、米国特許第５１８５７９６号（Ｗｉｌｓｏｎによる）は、伝送されるデータ共にインターリーブされる暗号化キー情報の提供と、信号ロスの際に再同期化を可能にするよう最適化されたセキュリティ方式とを開示する。キー自体は伝送されないが、送信サイトと受信サイトにおいて記憶される。米国特許第６０５２４６６号と第５１８５７９６号とに開示されたような方法は、いくつかの種類のデータ転送アプリケーションに適している。しかし、デジタル動画情報の配信や伝送に関して、これらの方法は、最良の解決法とは言えない。データの安全性を最大にし、全体の復号化速度を上げるために、キーまたはキー生成データと、キーの索引付けおよび同期化情報とを、別々に、データストリームから提供することが好ましい。動画とビデオデータに多重キーが使用される場合、ブロック内のデータの暗号化と、個々の動画またはビデオフレームとの間に、何らかの対応（上述の開示において対処されない）があれば好ましい。これについては後で述べる。

【００１４】ブロック内のデータを処理する方法の一例として、米国特許第６０２１３９１号（Ｓｈｙｕによる）は、個々の任意の長さのデータセグメントを処理することにより、データストリームを暗号化する方法を開示する。従って、個々のデータセグメントが、別々のキーとアルゴリズムを用いて、別々に暗号化される。その別々のキーとアルゴリズムは、データストリームの一部であるセグメントヘッダにおいて特定される。ここで再び、暗号化キーと暗号化アルゴリズムは、データストリーム自体において識別される。これは、暗号化キーを別個に提供する方法と比較すると、欠点といえる。上述と同様の理由で、データセグメントヘッダの明確な識別は、いくつかのアプリケーションにおいて有効でありうるが、例えば動画アプリケーションにおいて、映像や音声データを表示するデータストリームに対しては都合が悪い。

【００１５】データストリームを更に効率良くまたは安全に暗号化する別の方法が提案されている。対称キーの効率的な再利用のためのキー管理と使用の解決法の例の1つとして、米国特許第５４３８６２２号（Ｎｏｒｍｉｅ等による）は、オフセット値を提供する方法を開示する。そのオフセット値は、伝送されるシステムによって暗号化され、その後、暗号化／複号化のためのキーにおける「据え置き」スタート地点を特定するために使用される。キー自体は秘密キーと初期化ベクトルとから生成される。オフセット値が与えられると、復号化プロセッサは、復号処理において、オフセット値が示すキーの部分を使用できる。この方法により、可変オフセット値が、同じキーに、数回割り当てられ、効率的にキーを交換でき、また、暗号化する毎にキーの異なる部分が使用されるため、認可されない視聴者による反復パターンの解読が困難になる。ただ、この方法により、オフセット値が、送信機／受信機において生成されるキーに割り当てられ、暗号化／複号化毎に、その生成されたキーの大部分が破棄される必要があることに注意してほしい。さらに、そのキーの一部は、各々の暗号化処理で同じであってよいので、結局、単に全く異なるキーを提供する方法に比べて、より安全であるとは言えない。

【００１６】ビデオデータのブロックが暗号化される一例として、米国特許第６０２１１９９号（Ｉｓｈｉｂａｓｈｉによる）は、ＭＰＥＧ２のビデオデータストリームの暗号化方法を開示する。ＭＰＥＧ２（Ｍｏｔｉｏｎ Ｐｉｃｔｕｒｅ Ｅｘｐｅｒｔｓ Ｇｒｏｕｐの規格）は、ビデオデータを、Ｉフレームが参照フレームとして機能する一連のフレームとして記憶する。また、別のＭＰＥＧフレーム（ＰおよびＢ従属フレーム）は、正確に解釈されるために、Ｉフレーム（内部コード化されたスタンドアローンフレーム）への参照を必要とする。イシバシ（Ｉｓｈｉｂａｓｈｉ）による特許においては、データストリームのこれらの不可欠なＩフレームだけが暗号化される。これは、Ｉフレームの復号化が実行されるまで、データストリームにおけるその他の任意のビデオ

データの使用を効果的に妨げる。この方法には利点もあるが、暗号テキストデータストリームにおけるフレームの境界が明確なままであり、データのセキュリティ面で不利であるために採用できない。暗号テキストデータストリーム内の、どの定義するフレームヘッダまたは同期化文字をもマスクし、データストリーム内の全てのデータを安全に暗号化することが最善の方法であろう。この方法における全体の安全性は、単にＩフレームの暗号化にかかっている。この選択的暗号化により操作は単純化され、暗号化の所要時間も最小となるが、一方で、この選択的符号化は、単一Ｉフレームの認可されない復号化が、同様に、他のＰおよびＢのフレームへのアクセスを容認するので不利である。

【００１７】記録媒体の配信に対するコピー保護方式は、動画データやその他のデータストリームの安全な記憶と配信に対する要求を満たすような解決法を提示しない。例えば、米国特許第６０２８９３２号（Ｐａｒｋによる）または米国特許第５９６３９０９号（Ｗａｒｒｅｎ等による）において開示されるような方式は、再生やコピーを不可能にする、または、抑止するが、特定の宛先ハードウェアに関してある進んだ知識を必要とするので、デジタル動画アプリケーションにとって実用的でない。米国特許第６０１６３４８号（Ｂｌａｔｔｅｒ等による）において開示されるようなペイパービュー方式は、挿入可能なＩＳＯ７８１６－３対応スマートカードを使ってビデオプログラムへ条件付のアクセスを行う復号コードを提供する。しかし、この配列は、データアクセスとアルゴリズム識別の提供に限られる。

【００１８】従来の手法は、安全な暗号化、および、受信サイトに提供される暗号化キーの配信や同期化に対するいくつかのニーズに応えるが、デジタル動画のプロバイダが要求するような、大容量のデータストリーム配信のセキュリティ要請に十分対応できるデータ暗号化解決法を提供しない。さらに、従来の方法は、編集、再始動および早送りの機能を可能にするデジタル動画データストリームのフレームごとのアクセスに対する特定の要求を満足させることはできない。そのため、データストリームにおける個々のブロックに多重暗号化キーを同期させる安全な暗号化装置および方法が必要である。その装置および方法は、デジタル動画アプリケーションにうまく応用できる。

【００１９】

【発明が解決しようとする課題】本発明の目的は、データストリームを複数の順次データブロックとして暗号化する装置と方法とを提供することである。その各々のブロックには、暗号化キーが割り当てられる。また、本発明の目的は、各々の暗号化キーを、対応するデータブロックに同期させる安全な方法を提供する装置および方法を提供することである。

【００２０】

【課題を解決するための手段】本発明のある側面によると、デジタルデータソースからデジタルデータ受信機へ、複数のデータブロックを安全に転送するデータ転送装置が提供される。この装置は、（ａ）各々の単一データブロックに対して、前記各々の単一データブロックに割り当てられる暗号化キー、および、前記暗号化キーと前記単一データブロックとの間の対応を示すブロック同期化索引を提供できる暗号化キー生成器と、（ｂ）前記各々の単一データブロックに対して、前記暗号化キー生成器からの前記暗号化キーを用いて、暗号化プロセスを実行する暗号化エンジンと、（ｃ）前記暗号化されたデータブロックを、前記暗号化エンジンから前記デジタルデータ受信機へ配信するデータ伝送チャンネルと、（ｄ）前記暗号化キーを、前記暗号化キー生成器から前記デジタルデータ受信機へ配信するキー伝送チャンネルと、（ｅ）前記ブロック同期化索引を、前記暗号化キー生成器から前記デジタルデータ受信機へ配信するブロック同期化データチャンネルとからなる。

【００２１】本発明のもう１つの特徴は、複数の暗号化キーの各々１つを、データの各々のブロックに相対的な可変オフセットを用いて、データの対応するブロックに索引付けすることである。

【００２２】データストリームを、デジタルデータソースからデジタルデータ受信機へ、安全に転送する本発明に係る方法は、（ａ）前記のデータストリームを、平均サイズと無作為に生成されたオフセットとに基づいて、各々のサイズが可変である複数の連続したデータブロックに分割するステップと、（ｂ）各々の連続するデータブロックに対して、暗号化キーを生成するステップと、（ｃ）前記の各々の連続するデータブロックを、前記の暗号化キーを用いて暗号化し、暗号化されたデータブロックを提供するステップと、（ｄ）前記の暗号化されたデータブロックを前記の暗号化キーに関連付ける同期化索引を生成するステップとからなる。

【００２３】また、デジタル動画像データストリームを、デジタルデータソースからデジタルデータ受信機まで、安全に転送する本発明に係る方法は、（ａ）前記のデジタル動画像データストリームを、複数のデジタル動画像データブロックに分割するステップと、（ｂ）複数の暗号化キーを生成するステップと、（ｃ）前記の複数のデジタル動画像データブロックの各々に対して、（１）前記の各々のデジタル動画像データブロックを、識別可能な（ｄｉｓｔｉｎｃｔ）暗号化キーを用いて暗号化し、暗号化されたビデオデータブロックを生成するステップと、（２）前記の暗号化されたデータブロックを、前記の暗号化されたデジタル動画像データストリームの一部として記憶するステップとからなるステップを繰り返すことにより、暗号化されたデジタル動画像データストリームを生成するステップと、（ｄ）前記の各々のデジタル動画像データブロックを、前記の各々の識別

可能な暗号化キーと関連付ける同期化索引を生成するステップと、（ｅ）前記の暗号化されたデジタル動画像データストリームを、前記のデジタルデータ受信機に提供するステップと、（ｆ）前記の同期化索引を、前記のデジタルデータ受信機に提供するステップとからなる。

【００２４】また、複数の暗号化キーを、対応する複数の暗号化されたデータブロックにマッピングする本発明に係る方法は、（ａ）前記の複数の暗号化キーを、前記の暗号化されたデータブロックとは別個に提供するステップと、（ｂ）マッピングアルゴリズムを前記の複数の暗号化キーに相関させる識別子を提供するステップとからなる。

【００２５】また、動画の暗号化されたデジタル動画像データブロックを復号化する本発明に係る方法は、デジタル動画像データフレームまたはデジタル動画像データフレーム成分の識別を提供するステップと、複数の暗号化キーから対応するキーを生成し、それを、前記のデジタル動画像データフレームまたはデジタル動画像データフレーム成分がその一部を形成するデジタル動画像データブロックの復号化に使用するステップとからなる。

【００２６】

【発明の効果】本発明は、暗号化されるブロックサイズを選択するフレキシブルな装置を提供する。これは、順に、データストリームに適用される暗号化キーの数を自由に選択することを可能にする。暗号化キーの数を最大にすれば、データの安全性は最高のレベルに保つことができる。同時に、配信方法により、提供されうる暗号化キーの数が制限を受ける場合がある。

【００２７】本発明のさらなる側面によると、データブロックの先頭に対してランダムオフセットを生成する方法が提供される。これにより、ブロックの境界を決定する面倒な操作と、次の暗号化キーが適用されるデータストリーム中の地点を正確に決定する面倒な操作とが不用になる。

【００２８】本発明のさらなる効果は、本発明が暗号化キーに必要なオーバーヘッドデータのサイズを最小にする効率的な方法を提供することである。このため、多数の暗号化キーは、伝送によって、または、着脱可能な記憶媒体に記録することによって、容易に配信できる。

【００２９】本発明のさらなる効果は、デジタル動画の安全な暗号化と伝送に適用されるとき、個々のフレームへのアクセスを可能にする暗号化方法を提供できることである。これにより、デジタル動画データストリームの、編集または放映される部分だけが、いつでも復号化される。

【００３０】

【発明の実施の形態】以下に、添付の図面を参照して、本発明の実施の形態について説明する。この説明は、特に、本発明による装置の一部を形成する要素、または、本発明による装置に直接的に関与する要素に対してなされる。特に図示または説明されない要素が多様な変形をとりうることは当業者に周知であることが理解されるべきである。

【００３１】以下の詳細な説明は、主として、デジタル動画の安全な伝送や記憶を提供する暗号化装置の使用法に関するものであることに注意するべきである。この使用方法は、本発明の好ましい実施の形態であるが、本発明がさらに広範囲に適用可能であり、特に、大容量のデータが配信サイトから１以上の受信サイトへ安全に転送されなければならない任意の場合に適用できることは、データ暗号化およびデータ伝送の当業者にとって明らかである。また、「データストリーム」という言葉を、任意のタイプの大容量データ転送を含む従来の意味で使用している。本出願の文章において、データストリームは、転送されるデータの全ユニットが多重ブロックにおいて暗号化されなければならないような十分なサイズを有する。その暗号化は、各々のブロックに対して同じキーを使用して、または、複数のブロックを暗号化するために複数のキーが使用される配列を使用して行われる。

【００３２】図１を参照すると、概して符号１０で示されるデータストリームの安全転送装置が示されている。ここでは、データ発信サイト１２からデータ宛先サイト１４へ、安全にデータストリームが転送される。デジタルデータソース１８は、ソースデータストリームを提供する。そのデジタルデータソース１８は、デジタルデータを出力する多数の装置のうち任意のものであってよい。例えば、デジタルデータソース１８は、入力としてフィルムを走査し、出力としてデジタルデータを提供するテレシネ装置からなってもよい。または、代わりに、デジタルデータソース１８は、中間のテレシネ装置を必要とせずにデータを提供するデジタルカメラからなってもよい。または、代わりに、デジタルソース１８は、ハードディスクのバンクのような大容量の記憶媒体（例えば、ＲＡＩＤアレイ）からなってもよい。デジタルデータソース１８は、入力されたデータストリームを、特定のアプリケーションに適用できる形式にフォーマットする。

【００３３】次に、圧縮エンジン２０は、その入力されたデータストリームを受信し、圧縮アルゴリズムを適用する。例えば、デジタル動画データの場合、入力されたデータストリームは、ＭＰＥＧ－２データとして圧縮される。ＭＰＥＧ－２ビデオデータは、複数のフレーム内に記憶される。各々のフレームは、Ｙ、Ｃｒ、Ｃｂという３つの色成分をもつ。（デジタル動画の表示には、産業規格として、ＭＰＥＧ－２または変形ＭＰＥＧ－２のフォーマットが推奨されるが、ＪＰＥＧまたはＪＰＥＧ－２０００といった他のデータフォーマットが利用可能であることに注目することは有益である。）データの圧縮が必要でない場合でも、動画データは圧縮されることが望ましい。

【００３４】結果として生じる圧縮されたデータストリームは、その後、暗号化エンジン２２に進む。圧縮エンジン２０と暗号化エンジン２２は、全てまたは部分的に、ハードウェア内で実行されてもよいし、または、適切なソフトウェアを搭載した高速コンピュータのワークステーションを使って実行されてもよい。そのソフトウェアは、本明細書を読んだ後であれば、当技術分野における通常の知識内で十分に開発できる。

【００３５】キーおよび同期生成器２８は、暗号化エンジン２２に、図２と図４に示すような各々のデータブロック２６に対する暗号化キー５０を提供する。後で述べるように、暗号化エンジン２２は、データブロック２６のサイズを、安全データストリーム転送装置１０のユーザが求める安全性に対して適切に暗号化できるようにする。従って、１以上の暗号化キー５０が暗号化エンジン２２に必要である。また、キーおよび同期生成器２８は、生成された各々の暗号化キー５０をその対応する１以上のデータブロック２６に関連付ける同期化索引を生成する。生成される同期化索引の特性およびその同期化索引に対して可能な実施の形態は、後に説明される。

【００３６】暗号化エンジン２２は、完了した暗号化されたデータブロック２６を、配信サイト記憶装置３０に一時的に記憶できる。この装置３０は、大容量記憶装置であるか、または、より一般的に、任意の適当な記憶装置またはメモリバッファであってよい。記憶装置３０に記憶またはバッファ処理されることが可能な圧縮された暗号テキストとしての、完了したデータストリームは、その後、データ伝送チャンネル３２を用いたデータ配信サイト１４への配信に利用できる。データ伝送チャンネル３２が多数の可能なデータ伝送機能を含むことはおおよそ理解できる。例えば、データ伝送チャンネル３２は、専用の高速電話線であってよい。または、代わりに、データ伝送チャンネル３２は、ＲＦ、マイクロ波または衛星による伝送を用いたデータ転送用の無線伝送チャンネルからなってもよい。また、データ伝送チャンネル３２は、コンピュータデータネットワーク、ローカルエリアネットワーク（ＬＡＮ）またはワイドエリアネットワーク（ＷＡＮ）からなってもよい。さらにもう１つの代替として、データ伝送チャンネル３２は、データ宛先サイト１４に転送されるＤＶＤまたは他の光ディスクのような大容量記憶媒体を使用してもよい。（図１において、文字Ｄは、サイト１２とサイト１４との間のデータ伝送チャンネル３２による接続を示している。）

【００３７】キーおよび同期生成器２８からのデータを転送する別個の機構を可能にするために、キー伝送チャンネル３４が備えられる。キー伝送チャンネル３４は、多数の可能なデータ伝送機構を含むとおおよそ理解してよい。例えば、キー伝送チャンネル３４は、電話線またはネットワークからなってもよい、または、ＲＦ、マイクロ波または衛星伝送を用いてキーデータを転送する無線伝送チャンネルからなってもよい。または、代わりに、キー伝送チャネル３４は、スマートカード、ディスケット、ＣＤ－ＲＯＭまたは他の記憶装置のような携帯記憶媒体を使用してもよい。比較的広範囲の帯域幅をもった伝送チャンネルまたは記憶装置を必要とするデータ伝送チャンネル３２とは異なり、キー伝送チャンネル３４は、数キロバイトのオーダーでデータを転送する必要があるだけである。（図１において、文字Ｋは、サイト１２とサイト１４との間のキー伝送チャンネル３４による接続を示している。）

【００３８】各々の暗号化キー５０を特定のデータブロック２６へマップする複数のブロック同期化索引を転送する別個の機構を可能にするために、ブロック同期化伝送チャンネル７８が備えられる。例えば、ブロック同期化伝送チャンネル７８は、電話線からなってもよい、または、ＲＦ、マイクロ波または衛星伝送を用いてブロック同期化データを転送する無線伝送チャンネルからなってもよい。または、代わりに、ブロック同期化チャンネル７８は、スマートカード、ディスケット、ＣＤ－ＲＯＭまたは他の記憶装置のような携帯記憶媒体を使用してもよい。比較的広範囲の帯域幅をもった伝送チャンネルまたは記憶装置を必要とするデータ伝送チャンネル３２とは異なり、ブロック同期化チャンネル７８は、数キロバイトのオーダーでデータを転送する必要があるだけである。（図１において、文字Ｂは、サイト１２とサイト１４との間のブロック同期化チャンネル７８による接続を示している。）単一の伝送チャンネルまたは記憶装置が、ブロック同期化チャンネル７８とキー伝送チャンネル３４の両方の代わりであってもよいことに注意するべきである。

【００３９】図１に示されるように、データ宛先サイト１４は、データ伝送チャンネル３２によって暗号テキストデータストリームを受信でき、キー伝送チャンネル３４によってキーデータを受信でき、ブロック同期化チャンネル７８によってブロック同期化データを受信できる。暗号テキストデータストリームは、データ伝送チャンネル３２の構造に従って、宛先サイト記憶バッファ３６によってバッファ処理できる。宛先サイト記憶バッファ３６は、多数の記憶装置またはメモリデバイスのうち任意の１つであってよい。例えば、宛先サイト記憶バッファ３６は、大容量の記憶装置であってよい、または、データがＤＶＤまたは光ディスク上に提供されるなら、ディスクドライブであってもよい。バッファ３６からの暗号テキストデータストリームは、復号化エンジン３８に入力される。その復号化エンジン３８は、通常、圧縮された平文データストリームを提供する所有権を主張できるハードウェア装置として具体化されるプロセッサである。復号化エンジン３８は、例えば、プロジェクタ４６の構成要素であってよい。宛先キーおよび同期生成器４０は、キー伝送チャンネル３４とブロック同期化チャ

ンネル７８とから入力されたデータを受信し、出力として、復号化エンジン３８に対して必要な暗号化キーと同期化データを提供する。解凍エンジン４２は、その平文のデータストリームに必要な任意のデータ解凍を行う。デジタル動画のアプリケーションの場合、データ操作およびフォーマット装置４４は、周知のアルゴリズムに従って、色補正や画像サイズの変更といったさらなる画像処理機能を提供できる。宛先サイト１４において平文動画データのアクセスを制限するために、データ操作およびフォーマット装置４４は、ビデオデータによって表現される画像をスクリーン上に投影するプロジェクタ４６の構成要素として実現されてもよい。

【００４０】図１は、本発明に最も関連するデジタルデータストリームの経路に沿った構成要素のみを図示していることに留意してほしい。データコンテンツや使用要件に応じて、デジタルデータストリームに他の多数の構成要素やプロセスが適用できることが理解されるべきである。例えば、キー伝送チャンネル３４やブロック同期化伝送チャンネル７８には、これらのチャンネル上で送信されるデータを暗号化することによって、追加のデータセキュリティを提供できる。

【００４１】暗号化キー５０のマッピング

一般的に、一連の多重データブロック２６に割り当てられる多重キー５０がある場合、ある形式のマッピング機構が必要とされる。（識別名または識別番号を用いるように）明示的に与えられようが、（データファイルまたはデータストリーム内の相対位置を用いるように）暗示的に与えられようが、あるタイプの同期化索引が使用され、データブロックを対応するキー５０にリンクさせるために必要とされる情報を提供する。

【００４２】図２を参照すると、データブロック２６に暗号化キー５０をマッピングする可能な例が示される。データブロック２６のサイズは任意であってよい。しかし、本開示はデジタル画像の暗号化に対してであるので、各々のデータブロック２６は、個々の圧縮されたフレーム５４に対応できる。さらに、図２に示されるように、各々のデータブロック２６は、個々の色分解（Ｙ、ＣｒまたはＣｂの成分）に対応してもよい。ここで、フレーム５４は、（ＪＰＥＧ－２０００における圧縮フレームのように）３色の色分解から成る。このような配列では、図２のキー＃１ａ、＃１ｂ、＃１ｃで示されるように、個々のキー５０は、各々のフレーム５４内で各々の色分解に割り当てられる。この配列は、図３に示されるような、暗号化キー５０を各々のフレーム５４成分に索引付けするキーマッピングテーブル５２またはアレイの構成とメンテナンスとを必要とする。

【００４３】本発明の目的は、個々のフレーム５４を暗号化／復号化する、図３に示されたものと実質的に同様の機能を提供することである。図９を参照すると、キーおよび同期生成器２８、４０によって実行されるプロセスの図式的なブロック図が示されている。このプロセスは、特定のフレーム５４にアクセスすることが必要なデータストリームに提供される暗号化キー５０を生成するプロセスである。このプロセスにおいて、キー抽出エンジン１６は、フレームまたはフレーム成分ＩＤ２４および（単に、何らかの方法において（ダミービットで）パッド処理され、インターリーブされ、または、スクランブル処理されることが可能な暗号化キー５０の順次リストであってよい）暗号化キー値を受信し、特定のフレーム５４に対して対応するキー５０を出力する。キー抽出エンジン１６は、各々のブロック２６に対して唯一のキー５０を生成するために、数学的または論理的プロセスを使用できる。図９に示されるプロセスについて、キー５０のブロック２６への（および、それに対応して、個々のフレーム５４への、または、個々のフレーム５４成分への）マッピングは、ブロック２６またはフレーム５４に関連付けられる、ある形式の明示的な同期化索引を用いて達成できる。または、簡単な場合には、同期化索引は、データストリーム内のフレーム５４の位置において暗示的であってよい（例えば、第５３７番目のキーを第５３７番目のフレームに割り当てる）。または、データストリームを暗号化する場合の安全性を高めるために、所有権を主張できるあるタイプのアルゴリズムが使用でき、その結果、暗示的な同期化索引付け機能が提供され、特定のブロック２６またはフレーム５４を、その対応するキー５０にマッピングできる。

【００４４】図２および図３は、相当数のキー５０を必要とする極端な例を示す。図４に示されるように、各々の暗号化キー５０が、多重フレーム５４から成るブロック２６に割り当てられるという代替の方法において効果があることは容易に理解できる。図４の例では、８つのフレーム５４が合体して１つのブロック２６になる。図４の配列に関して、各々のブロック２６は、単一の対応する暗号化キー５０を有する。好ましい実施の形態において、ブロック２６内の各々のフレーム５４は、ブロック２６に割り当てられた暗号化キー５０を用いて個別に暗号化される。図４の例を用いると、キーマッピングテーブル５２は、同期化索引として、（図３で示されたフレーム＃の代わりに）ブロック番号を使用でき、故に、そのサイズを実質的に縮小できることは明らかである。

【００４５】できるだけ多くのキー５０を提供すると同時に、キー５０とそれに関する同期化索引とに提供されなければならないデータの総量を削減できれば都合が良いことは理解できるだろう。図５を参照すると、代替のデータ構造６０が示される。そのデータ構造６０は、キーマッピングテーブル５２内の基本構造として採用され、図４に示される配列を用いたデータ構造から記憶要件を削減できる。図５の配列は、ブロック２６の（フレーム数の点で）任意のサイズを使用する実施例において最も有効である。図５の配列を使用すると、暗号化キー

５０は、先頭フレーム５４にマップされる。スタートブロックＩＤフィールド５６とスタート成分ＩＤフィールド５８は、まず、特定の暗号化キー５０が使用されるフレーム５４のためのマッピング情報を、２１ビットで提供する。その後、次に続くあるフレーム５４が、次のあるデータ構造６０によって識別されるまで、後続の（複数の）フレーム５４に対して、同一の暗号化キー５０が使用できる。この配列について、図3のテーブルは可変サイズであり、キー５０ごとに1つのデータ構造６０が使用される。図5の構造において、スタートブロックＩＤフィールド５６は、明示的な同期化索引として作用する。

【００４６】表2は、図5に示されたキー５０と同期化索引との配列に基づき、１３０分間の長さで毎秒３０個のフレームを使用する映画の場合に、異なるブロック２６サイズを用いて暗号化キー５０の値と同期化索引データとを記憶するために必要とされるデータバイトの相対的な数を比較する。これは、以下の式（１）で示される総数のフレーム５４を暗号化することを意味する。

【数１】

（１３０分／映画）×（６０秒／分）×（フレーム３０個／秒）＝フレーム２３４，０００個／映画　　（１）

【００４７】表2の「キー毎のオーバーヘッド」欄は、各々のフレーム５４に同期化索引を提供するために必要なビット数を示す。（フレーム数が２３４，０００といった）極端な場合において、このマッピングに対して総数１８ビット（2^{18}＝２６２，１４４なので）は十分である。それ故、この方式をより長い動画に適用可能にするために、１９ビットで十分である。あと２ビット追加すれば、以下の例のように、キー５０が適用するフレーム５４の成分を識別できる。

【表１】

ビットパターン	解釈
００	フレーム５４の全成分（Ｙ、Ｃｂ、Ｃｒ）に使用される暗号化キー５０
０１	ルーマ成分、Ｙに使用される暗号化キー５０
１０	Ｃｒ成分に使用される暗号化キー５０
１１	Ｃｂ成分に使用される暗号化キー５０

【００４８】表2のサイズは、規格ＤＥＳ（相当な演算時間と努力を費やせば、解錠される可能性がある）、または、トリプルＤＥＳアルゴリズム（本出願時点において、いまだ解錠されたことがない）を用いて、アルゴリズムによって記載される。

【表２】

表2　キー５０のデータ記憶に必要なバイト数の比較

アルゴリズム	最大キー長（ビット）	キーごとのオーバーヘッド（ビット）	ブロック２６毎に1個のキーであり、ブロック２６が下記のサイズの場合における、キー記憶に必要なバイト数			
			1フレーム成分（Ｙ、Ｃｒ、Ｃｂ）	1フレーム	１０フレーム	３０フレーム
ＤＥＳ	６４	２１	７，４５８，７５０	２，４８６，２５０	２４８，６２５	８２，８７５
トリプルＤＥＳ	１９２	２１	１８，６９０，７５０	６，２３０，２５０	６２３，０２５	２０７，６７５

【００４９】キー伝送チャンネル３４（図１）の実施における自由度を最大にするため、キー５０データ記憶に対するバイト数を削減する一方、同時に、十分な数のキー５０を利用し、データストリームに対する所望レベルのセキュリティを提供することは効果がある。例えば、１枚のスマートカードに暗号化キー５０を提供するために、データ量は、一般的に、８Ｋバイト以下でなければならない。従って、データ記憶空間を効率的に使用するキーの同期化を提供するという代替の手法には効果があることがわかる。本発明で使用されるこのような手法は、後で説明される。

【００５０】また、使用される各々のタイプの暗号化アルゴリズムでキーマッピングをサポートするために、表２の計算に含まれない追加のオーバーヘッドビットが必要である。

【００５１】また、表２に記載されるＤＥＳまたはトリプルＤＥＳのアルゴリズム以外に、好ましいアルゴリズムがあることに注目することは有効である。例えば、エクスポート制約により、暗号化に１以上の代替アルゴリズムを採用することは効果的である。例えば、特に他の補償セキュリティ対策が採られれば、より安全性の低いアルゴリズムが使用できる。ＤＥＳまたはトリプルＤＥＳ暗号化よりも安全性の低いアルゴリズムを使用する場合、その対策の一例として、より多数のキー５０使用すれば、ある程度、補償できる。

【００５２】キー５０の配信構造

効率的かつフレキシブルにデータを転送するために、キー同期化索引をできるだけコンパクトにすることが有益であることは明らかであろう。このため、本発明は、図６に示されるキーファイル７０のデータ構造を提供する。図１を再び参照すると、キーファイル７０は、暗号化キー５０とキー同期化索引データを、データ発信サイト１２からデータ宛先サイト１４へ配信する。

【００５３】キーファイル７０の構造を用いると、ヘッダフィールド６２は、（映画や映画館の名称などの）そのデータに関する一般的な情報を含み、暗号化タイプを特定する。同期化フィールド６４は、個々のキー５０を、ブロック２６または、相応して、フレーム５４にリンクさせるために使用される同期化索引情報を含む。キーオーバーヘッドフィールド６６は、キーフィールド６８からキー５０を得るために必要な情報を提供する。また、キーオーバーヘッドフィールド６６は、キーフィールド６８においてキー５０がどのように配列されるか、または、ブロック２６がどのように構成されるかを示すために使用できる。キーオーバーヘッドフィールド６６における種々の情報は、キーのインターリーブ、パッド処理またはダミービットの追加のような使用される技術

$$2^{m_1+1}-1$$

（擬似ランダム数を生成する技術において知られているように、次元が（m_1 +1）ビットのＬＦＳＲは、（m_1 +1）次の多項式によって特定でき、m_1 ビットの二進数で表される。）それ故、生成される擬似ランダム値は、後で説明するキー同期化方式において使用されるオフセットを提供するために使用できる。

【００５５】本発明において使用されるように、キーファイル７０を効率的に使用すれば、キー５０をデータブロック２６に同期化するために必要とされるオーバーヘッドを大幅に削減できることに注意するべきである。例えば、図６に示される手法は、多数のキー５０をデータブロック２６に同期化するために４０ビットのオーバーヘッドを利用するだけである。従って、例えば、全デジタル動画に対して、十分な同期化索引データを提供するために４０ビットが使用できる。図５と表２に示された手法とは対照的に、２１ビットの同期化索引データが、各々の暗号化キー５０のオーバーヘッドとして必要とされる。

【００５６】キーファイル７０を使ったキーの同期化方式

最小限のサイズでありながら、データストリームを高い安全性をもって暗号化するために十分なキー５０を含むことができるキーファイル７０を提供するために、まず、キー伝送チャンネル３４と所望の安全性レベルとによって課される全体サイズの制約に基づいて、キー５０の数が計算される。約８Ｋバイトのメモリ容量を備えたについてのデータを含む。または、代わりに、キーオーバーヘッドフィールド６６は、キーフィールド６８内の対応するキー５０を探し出すために使用されるアルゴリズムを特定できる。キーフィールド６８は、任意の数のキー５０を含むことができるが、その数は、主に、ファイルサイズやセキュリティ要件によって制約される。

【００５４】好ましい実施の形態において、同期化フィールド６４は、２つの成分（m_1 ，m_2 ）からなるｍビットを含む。同期化索引データを提供するために、ビットm_1 が使用され、ＬＦＳＲ（線形フィードバックシフトレジスタ）の構造を特定する。ＬＦＳＲは、データ暗号化技術における周知の技術を用いて（復号化エンジン３８と暗号化エンジン２２内の）擬似ランダム数を生成する。ビットm_2 は、そのＬＦＳＲのシードとして使用されるランダム数を提供する。例えば、m_1 +m_2 ＝１９＋２１＝４０ビットという値を使えば、ＬＦＳＲを使って、キー同期化の１，０４８，５７５擬似ランダム値が生成できる。１，０４８，５７５という値は、以下の式で計算される。

【数２】

現在のスマートカードのアプリケーションについて、キーファイル７０は、（トリプルＤＥＳ暗号化による）図６のデータ構造配列を用いて、約３００個のキーを含むことができる。つまり、キー５０が再利用されない最も単純な手法を用いれば、これは、約３００個のデータブロック２６を提供することを意味する。

【００５７】次のステップは、暗号化されたデータブロック２６毎に、フレーム５４（または、フレーム５４の成分）の数を計算することである。暗号化するために、データストリームを、均等なサイズのブロック２６に分割することが可能である。これは、単に、フレーム５４の総数を、キー５０の総数で割ればよい（残余バイトを扱うために、異なるサイズのブロック２６を１個残す）。同サイズのブロック２６を使用することは簡単な手法であるが、さらに安全性の高い解決法は、ブロック２６のサイズにいくらかのランダム性を導入することである。図７を参照すると、ランダムなオフセット７６を割り当てることにより、安全性がさらに増す。それは、各々のキー５０を用いたデータストリーム７２（好ましい実施の形態において、データストリーム７２は、動画データそのものである。）の暗号化／復号化を、均等な間隔に並んだブロック境界７４からオフセットされたフレーム５４で開始または終了させる。上述したように、これは、安全性の効果を提供し、未認可の受信者が、個々のブロック２６の始点と終点とを決定すること、従って、キー５０に対するフレーム５４の対応を決定するこ

とを、より困難にする。

【００５８】ランダムオフセット７６を適用する前に、データストリーム７２内のブロック境界７４を決定するために、各々の暗号化ブロック内で、まず、フレーム５４数の平均を決定する必要がある。これは、フレーム５４の総数（または、フレーム５４の成分、Ｙ、Ｃｒ、Ｃｂの数）Ｍを、利用可能な暗号化キー５０の総数Ｎによって割り、そのフロア関数（割算による整数値を提供し、任意の残った端数を削除する）を取ることにより達成される。この計算は、ブロックの境界値７４を提供する。

【数３】

$$\text{フレーム数の平均 } (\overline{B}) = \left\lfloor \frac{\text{フレームの総数 (M)}}{\text{暗号キーの総数 (N)}} \right\rfloor \qquad (3)$$

（図７において、 $0,\overline{B},2\overline{B},3\overline{B},4\overline{B}$ で例示される）

【００５９】その後、ランダムオフセット７６（図７の O_i 、ここで、ｉは特定のデータブロック２６を示す）は、（例えば、線形フィードバックシフトレジスタのような）擬似ランダム数生成を用いて計算される。このランダムオフセット７６は、以下の式（４）を満足するように計算される。

【数４】

$$\left(-\left\lfloor \frac{\overline{B}}{2} \right\rfloor \le O_i \le \left\lfloor \frac{\overline{B}}{2} \right\rfloor\right) \qquad (4)$$

ここで、（$1 \le i \le N$）

【００６０】ランダムの量を制限する実質的な理由がありうる。故に、ブロック２６は適正にサイズが決められる。例えば、もしブロック２６のサイズが完全にランダムであれば、あるブロック２６は、単に、数個のフレーム５４しか含まず、他のブロックは、多数のフレーム５４を含む可能性がある。このような配列は、固有の不都合を有する。例えば、大容量のブロック２６に対するキー５０の発見は、データの大部分の復号化を可能にする。容量の小さいブロック２６に対するキー５０の発見、つまり、「解錠」は、特に、容量の小さいブロック２６に既知の画像コンテンツがあるなら、より実行し易い。それ故、オフセット７６のサイズを制限する最も実用的な手法は、上述したようなブロック２６を適正サイズに保つことであることがわかる。

【００６１】データブロック２６の基本ユニットは、データストリーム７２中のデータのタイプに依存していることに注意するべきである。デジタル動画について、好ましい実施の形態において最も実用的な配列は、フレーム５４を基本ユニットとして使用することである。これは、オフセット７６が、フレーム５４のユニットにおいて適用されて処理されることを意味する。（他の配列も可能であるが、デジタル画像データに対するフレームごとのアクセスが必要とされる。）

【００６２】キーファイル７０の生成

図６を再び参照すると、キーファイル７０は、暗号化された各々のデータブロック２６に対するキー５０を含むキーフィールド６８を備えている。同期化フィールド６４は、ランダムオフセット７６を生成するシード値を含んでもよい。復号化エンジン３８は、同期化フィールド６４と、キーフィールド６８におけるキー５０の値とを使って、各々のキー５０をそれに対応するランダムオフセット７６を含むデータブロック２６にマップするテーブルまたはマトリックスを、メモリに生成する。その後、復号化エンジン３８は、その復号化操作を同期化するために、メモリからのデータを使う。

【００６３】キーファイル７０は、スマートカードまたは他の着脱可能な媒体上の各々の映画サイトに提供できる。または、キーファイル７０は、例えば公開キー暗号化を使用して、各々のサイトに安全に転送できる。いずれにしても、更に安全性を高めるために、キーファイル７０は、好ましくは、暗号化される。

【００６４】図８を参照すると、データ発信サイト１２において実行される、ランダムオフセット７６をもつ多重キー５０を備えたデータストリーム７２の暗号化プロセスの流れ図が示されている。最初のステップにおいて、まず、基本ブロックのサイズ（式（３）におけるフレーム数の平均）が計算され、上述したように、キーファイル７０におけるキー５０の数に対する容量が与えられる。その後、平文データの各々のデータブロック２６について、オフセット７６とキー５０が計算される。データブロック２６は暗号化され、配信サイト記憶装置３０に記憶される。キー５０とオフセット７６データは、キーおよび同期生成器２８によって、一時的に安全に記憶される。全ての平文データが暗号化されるまで、このプロセスが繰り返される。その後、キーファイル７０は、キーおよび同期生成器２８によって、記憶されたキー５０と同期化索引データ（つまり、上述の方法で提供された、ＬＦＳＲ構造とと初期化シード）とからアセンブルされる。その後、記憶装置３０からのデータは、記録媒体で記録されてもよいし、データ宛先サイト１４に

伝送されてもよい。

【００６５】特にいくつかの好ましい実施の形態を参照しながら本発明について説明してきたが、本発明の範囲から逸脱することなく多様な変形が可能であり、好ましい実施の形態における要素を同質のもので代用することも可能であることが当業者に理解されよう。例えば、キーファイル７０のファイル構造は、追加の復号化情報を含むように拡張できる。また、セキュリティを強化するために、キーファイル７０内のキー５０を、例えばランダムなビット値でパッド処理したり、所定の様式でインターリーブしたり、配列することが可能である。随意的に、ランダムオフセット７６の生成に必要な値を提供するために、別々の手段を用いることができる。例えば、ＬＦＳＲのシード値は、個別のファイル、または、復号化する別のタイプのキーの役割を果たす個別の伝送物において提供されてもよい。または、代わりに、記憶装置は、キー、または、データ宛先サイトの読取用に提供されるＲＦＩＤ成分のようなオフセット生成データが提供されてもよい。

【００６６】キーファイル７０は、単一ファイルとして提供される必要はないが、ばらばらに分割提供され、それら各々が個別に暗号化され、異なる形式で、または、異なる伝送チャンネルを介して提供されれば効果的である。

【００６７】これまでの詳細な説明は、映像成分の暗号化における本発明の実施方法を開示するが、デジタル動画ファイルに添付する音声データの復号化にも同様の方式が使用できる。

【００６８】また、本発明は、リアルタイムの映像／音声プログラムの再生アプリケーションに、効果的に適用できる。例えば、キーファイル７０へのデータは、映像／音声プログラムの伝送に先駆けて、データ宛先サイト１４に配信または伝送される。その後、プログラムデータが受信されると、ライブの映像／音声データストリームが復号化される。

【００６９】関連の実施の形態において、セキュリティを向上させるために、データブロック２６を非順次形式で提供できる。または、データ伝送チャンネル３２は、データブロック２６を転送する平行チャンネルを含んでもよい。個々の平行チャンネルは、バンド幅がより小さく低コストである。データブロック２６は、ランダムな順序で伝送され、宛先サイトで正しい順序に再配列されてもよい。

【００７０】それ故、以下に、データストリームを、複数の順次データブロックとして暗号化および／または復号化する装置と方法を示す。ここで、各々のブロックは、割り当てられた暗号化キーを備える。また、以下に、各々の暗号化キーを対応するデータブロックに安全に同期化する方法を示す。

【００７１】１．複数のデータブロックを、デジタルデータソースからデジタルデータ受信機まで、安全に転送するデータ転送装置であって、（ａ）前記複数のデータブロックの各々の単一データブロックに割り当てられる暗号化キー、および、前記暗号化キーと前記単一データブロックとの間の対応を示すブロック同期化索引を提供する暗号化キー生成器と、（ｂ）前記各々の単一データブロックに対して、前記暗号化キー生成器からの前記暗号化キーを用いて、暗号化されたデータブロックを生成する暗号化エンジンと、（ｃ）前記暗号化されたデータブロックを、前記暗号化エンジンから前記デジタルデータ受信機へ配信するデータ伝送チャンネルと、（ｄ）前記暗号化キーを、前記暗号化キー生成器から前記デジタルデータ受信機へ配信するキー伝送チャンネルと、

（ｅ）前記ブロック同期化索引を、前記暗号化キー生成器から前記デジタルデータ受信機へ配信するブロック同期化データチャンネルとからなる装置。

２．前記のデジタルデータ受信機が、前記の暗号化キーに応答する復号化エンジンを備え、前記の暗号化エンジンと復号化エンジンとが、対称暗号化を備える項目１に記載の装置。

３．前記の単一データブロックのサイズが各々異なる項目１または項目２に記載の装置。

４．前記の単一データブロックがビデオデータからなる項目１から項目３のいずれかに記載の装置。

５．前記のデータ伝送チャンネルが無線伝送ネットワークである項目１から項目４のいずれかに記載の装置。

６．前記のデータ伝送チャンネルが専用電話サービスを利用する項目１から項目４のいずれかに記載の装置。

７．前記のデータ伝送チャンネルが携帯記憶媒体を利用する項目１から項目４のいずれかに記載の装置。

８．前記のデータ伝送チャンネルがコンピュータデータネットワークを利用する項目１から項目４のいずれかに記載の装置。

９．前記のデータ伝送チャンネルがローカルエリアネットワークを利用する項目１から項目４のいずれかに記載の装置。

１０．前記のデータ伝送チャンネルがワイドエリアネットワークを利用する項目１から項目４のいずれかに記載の装置。

１１．前記のブロック同期化伝送チャンネルがスマートカードを利用する項目１から項目１０のいずれかに記載の装置。

１２．前記のブロック同期化伝送チャンネルが携帯記憶媒体を利用する項目１から項目１０のいずれかに記載の装置。

１３．前記のブロック同期化データが暗号化されている項目１から項目１２のいずれかに記載の装置。

１４．前記のキー同期化伝送チャンネルがスマートカードを利用する項目１から項目１３のいずれかに記載の装置。

１５．前記のキー同期化伝送チャンネルが携帯記憶媒体を利用する項目１から項目１３のいずれかに記載の装置。
１６．前記のキー同期化データが暗号化されている項目１から項目１５のいずれかに記載の装置。
１７．前記の単一データブロックが圧縮されている項目１から項目１６のいずれかに記載の装置。
１８．前記のブロック同期化索引が、擬似ランダム数生成器を用いて計算される項目１から項目１７のいずれかに記載の装置。
１９．前記の擬似ランダム数生成器が線形フィードバックシフトレジスタである項目１８に記載のデータ搬送装置。
２０．データストリームを、デジタルデータソースからデジタルデータ受信機へ、安全に転送する方法であって、（ａ）前記データストリームを、平均サイズと無作為に生成されたオフセットとに基づいて、各々のサイズが可変である複数の連続したデータブロックに分割するステップと、（ｂ）各々の連続するデータブロックに対して、暗号化キーを生成するステップと、（ｃ）前記各々の連続するデータブロックを、前記暗号化キーを用いて暗号化し、暗号化されたデータブロックを提供するステップと、（ｄ）前記暗号化されたデータブロックを前記暗号化キーに関連付ける同期化索引を生成するステップとからなる方法。
２１．前記の暗号化されたデータブロックを提供するステップが、前記の暗号化されたデータブロックを記録媒体に記録するステップを含む項目２０に記載の方法。
２２．前記の記録媒体が磁気記憶技術を使用する項目２１に記載の方法。
２３．前記の記録媒体が光学記憶技術を使用する項目２１に記載の方法。
２４．さらに、前記の暗号化されたデータブロックを前記のデジタルデータ受信機に伝送するステップを含む項目２０から項目２３のいずれかに記載の方法。
２５．さらに、前記の暗号化キーを暗号化するステップを含む項目２０から項目２４のいずれかに記載の方法。
２６．さらに、前記の暗号化されたデータブロックを、非順次で前記の受信サイトへ伝送するステップを含む項目２０から項目２５のいずれかに記載の方法。
２７．前記のデータストリームがデジタル動画像データからなる項目２０から項目２６のいずれかに記載の方法。
２８．前記のデータストリームを分割するステップにおいて、ランダムに生成されるオフセット値が、データブロックのサイズを決定するために生成される項目２０から項目２７のいずれかに記載の方法。
２９．デジタル動画像データストリームを、デジタルデータソースからデジタルデータ受信機まで、安全に転送する方法であって、（ａ）前記デジタル動画像データストリームを、複数のデジタル動画像データブロックに分割するステップと、（ｂ）複数の暗号化キーを生成するステップと、（ｃ）前記複数のデジタル動画像データブロックの各々に対して、（１）前記各々のデジタル動画像データブロックを、識別可能な暗号化キーを用いて暗号化し、暗号化されたビデオデータブロックを生成するステップと、（２）前記暗号化されたデータブロックを、前記暗号化されたデジタル動画像データストリームの一部として記憶するステップとからなるステップを繰り返すことにより、暗号化されたデジタル動画像データストリームを生成するステップと、（ｄ）前記各々のデジタル動画像データブロックを、前記各々の識別可能な暗号化キーと関連付ける同期化索引を生成するステップと、（ｅ）前記暗号化されたデジタル動画像データストリームを、前記デジタルデータ受信機に提供するステップと、（ｆ）前記同期化索引を、前記デジタルデータ受信機に提供するステップとから成る方法。
３０．前記のデジタル動画像データストリームを、複数のデジタル動画像データブロックに分割するステップが、さらに、前記の各々のデジタル動画像データブロックの先頭フレームを設定するために使用されるオフセット値を生成するステップを含む項目２９に記載の方法。
３１．前記のデジタル動画像データストリームを複数のデータブロックに分割するステップが、基本ユニットとして、デジタル動画像フレームを使用する項目２９または項目３０に記載の方法。
３２．同期化索引を生成するステップが、さらに、前記の同期化索引を暗号化するステップを含む項目２９から項目３１のいずれかに記載の方法。
３３．前記の暗号化されたビデオデータストリームを前記のデジタルデータ受信機に提供するステップが、前記の暗号化されたビデオデータストリームを伝送するステップからなる項目２９から項目３２のいずれかに記載の方法。
３４．前記の暗号化されたビデオデータストリームを前記のデジタルデータ受信機に提供するステップが、前記の暗号化されたビデオデータストリームを記憶媒体に記録するステップからなる項目２９から項目３２のいずれかに記載の方法。
３５．前記の同期化索引を前記のデジタルデータ受信機に提供するステップが、前記の同期化索引を伝送するステップからなる項目２９から項目３４のいずれかに記載の方法。
３６．前記の同期化索引を前記のデジタルデータ受信機に提供するステップが、前記の同期化索引を記憶媒体に記録するステップからなる項目２９から項目３４のいずれかに記載の方法。
３７．複数の暗号化キーを、対応する複数の暗号化されたデータブロックにマッピングする方法であって、
（ａ）前記複数の暗号化キーを、前記暗号化されたデー

タブロックとは別個に提供するステップと、（ｂ）マッピングアルゴリズムを前記複数の暗号化キーに相関させる識別子を提供するステップとからなる方法。
３８．前記の複数の暗号化キーが非順次にインターリーブされる項目３７に記載の方法。
３９．さらに、前記の複数の暗号化キーを、ダミービットを用いてパッド処理するステップを含む項目３７または項目３８に記載の方法。
４０．前記の暗号化されたデータブロックがデジタル動画像データブロックとからなり、そのデジタル動画像データブロックは、デジタル動画像データフレームまたはデジタル動画像データフレーム成分の識別を提供すること、および、複数の暗号化キーから対応するキーを生成し、それを、フレームまたはフレーム成分がその一部を構成するブロックの復号化に使用することによって復号化される項目３７から項目３９いずれかに記載の方法。
４１．各々のデジタル動画像データブロックが、動画のデジタル動画像データフレーム成分である項目４０に記載の方法。
４２．各々のデジタル動画像データブロックが、動画のデジタル動画像データフレームである項目４０に記載の方法。
４３．前記の暗号化されたデータブロックの復号化が、前記のデジタル動画像データによって表示される画像をスクリーン上に投影するデジタル動画像プロジェクタにおいてなされる項目４０から項目４２のいずれかに記載の方法。
４４．前記のデジタル動画像データブロックが、圧縮された形式の動画のデータからなり、前記の動画全体が暗号化される項目４０から項目４３のいずれかに記載の方法。
４５．前記のデジタル動画像データブロックが、ＭＰＥＧ形式の圧縮法を用いて圧縮され、内部コード化されたスタンドアロンフレームと従属フレームＰ、Ｂが形成され、その内部コード化されたフレームと、フレームＰ、Ｂが暗号化される項目４０から項目４３のいずれかに記載の方法。
４６．前記のデジタル動画像データフレームが複数の色成分からなり、その色成分の１つのデータのみが暗号化される項目４２に記載の方法。
４７．前記の暗号化された色成分が、１より大きなビット深さによって示され、その色成分データの１つのビットプレーンのみが暗号化される項目４６に記載の方法。
４８．動画の暗号化されたデジタル動画像データブロックを復号化する方法であって、デジタル動画像データフレームまたはデジタル動画像データフレーム成分の識別を提供するステップと、複数の暗号化キーから対応するキーを生成し、それを、前記デジタル動画像データフレームまたはデジタル動画像データフレーム成分がその一部を形成するデジタル動画像データブロックの復号化に使用するステップとからなる方法。
４９．各々のブロックが、前記の動画のデジタル動画像データフレーム成分である項目４８に記載の方法。
５０．各々のブロックが、前記の動画のデジタル動画像データフレームである項目４８に記載の方法。
５１．さらに、前記の暗号化されたデータブロックを、前記のデジタル動画像データによって表示される画像をスクリーン上に投影するデジタル動画像プロジェクタにおいて復号化するステップを含む項目４８から項目５０のいずれかに記載の方法。
５２．前記のデジタル動画像データブロックが、圧縮された形式の動画のデータからなり、その動画全体が暗号化される項目４８から項目５１のいずれかに記載の方法。
５３．前記のデジタル動画像データブロックが、ＭＰＥＧ形式の圧縮法を用いて圧縮され、内部コード化されたスタンドアロンフレームと従属フレームＰ、Ｂが形成され、それら内部コード化されたフレームとフレームＰ、Ｂが暗号化される項目４８から項目５１のいずれかに記載の方法。
５４．デジタル動画像データフレームが複数の色成分からなり、その色成分の１つのデータのみが暗号化される項目４８から項目５１のいずれかに記載の方法。
５５．前記の暗号化された色成分のデータが、１より大きな１ビット深さによって示され、その色成分データの１以上であるが全部より少ないビットプレーンが暗号化される項目５４に記載の方法。
５６．デジタル動画像データフレームが、複数の色成分からなり、前記の色成分のデータが暗号化される項目４８から項目５１のいずれかに記載の方法。
５７．各々の色成分が、１より大きな１ビット深さによって示され、各々の色成分データの１以上であるが全部より少ないビットプレーンが暗号化される項目５６に記載の方法。
５８．ブロックの境界が、フレーム内の対応する位置からの可変オフセットを有する項目４８から項目５７のいずれかに記載の方法。
５９．暗号化キーに相対的な対応情報を提供する索引が、暗号化されたデータブロックの暗号テキストを提供するチャンネルとは別のチャンネルにおいて提供される項目４８から項目５８のいずれかに記載の方法。
６０．単一のデータブロックが、動画の複数のフレームを示す項目４８に記載の方法。
６１．データブロックのサイズが各々異なる項目６０に記載の方法。
６２．ブロックの境界が、フレーム内の対応する相対位置からの可変オフセットを有する項目６１に記載の方法。
【００７２】本発明においては、上記の指示に従った多様な修正と変形が可能である。それ故、本請求項の範囲

を逸脱することなく、上記で説明した以外の方法でも本発明の実施が可能であることが理解されよう。

【図面の簡単な説明】

【図１】　本発明によるデジタル動画アプリケーションにおいて使用されるデータストリームを安全に転送する装置を図式的に示す図。

【図２】　本発明によるデジタル動画に関するフレームの個々の成分に対するキー割り当てを図式的に示す図。

【図３】　本発明によるデジタル動画に関するフレーム成分と対応するキーとの表を作る基本的なキー割り当てテーブルの一例を示す図。

【図４】　本発明によるデジタル動画に関するフレームのブロック内における複数のフレームへのキー割り当てを図式的に示す図。

【図５】　本発明による単一キーに関する略式暗号化キー割り当て構造の一例を示す図。

【図６】　同期化データを含む、本発明による多重キーに関する暗号化キー割り当て構造を示す図。

【図７】　本発明による暗号化ブロックに関する無作為に生成されたオフセット値の使用を示す図。

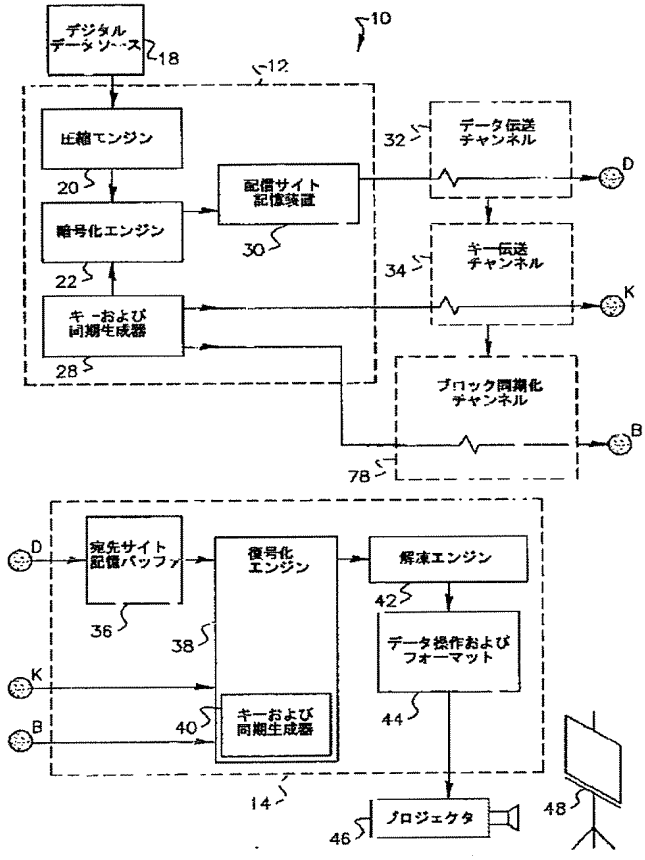
【図８】　本発明によるデータ暗号化とキー生成の全工程を示す流れ図。

【図９】　本発明による複数のデータブロックを利用したキー生成と同期化の１つの工程を示す図式的なブロック図。

【符号の説明】

１０　安全データストリーム転送装置
１２　データ発信サイト
１４　データ宛先サイト
１８　デジタルデータソース
２０　圧縮エンジン
２２　暗号化エンジン
２８、４０　キーおよび同期生成器
３０　配信サイト記憶装置
３２　データ伝送チャンネル
３４　キー伝送チャンネル
３６　宛先サイト記憶バッファ
３８　復号化エンジン
４２　解凍エンジン
４４　データ操作およびフォーマット
４６　プロジェクタ
７８　ブロック同期化チャンネル

【図１】

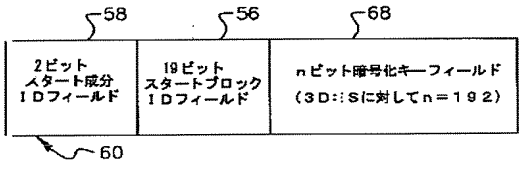


【図３】

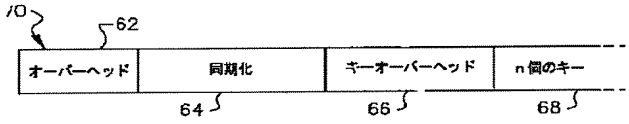
フレーム　#	暗号化キー
1a	12368926518651266687...
1b	726539827/63776723445...
1c	8923343247128937833346...
2a	/6326742678945633766...
2b	453982777542/79080...
2c	2338/745824675678764...
3a	454345344348768769999...
3b	436535390800948764387...
...	...

50
52

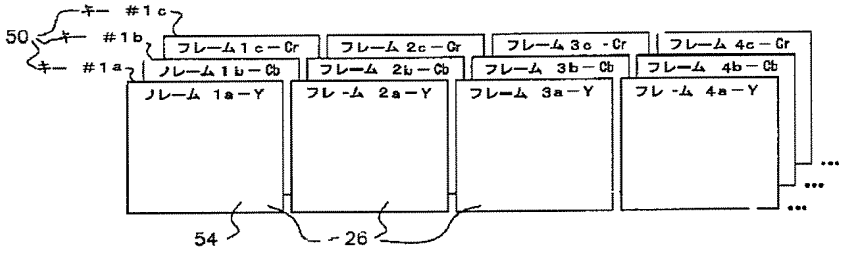
【図５】



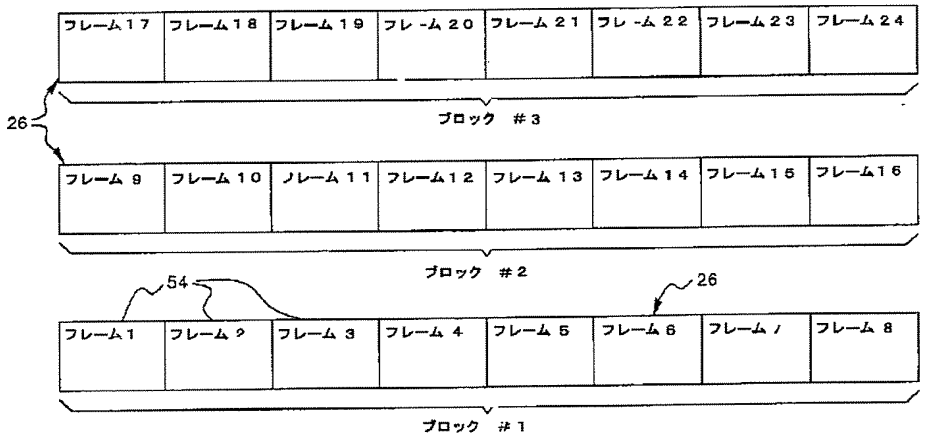
【図６】



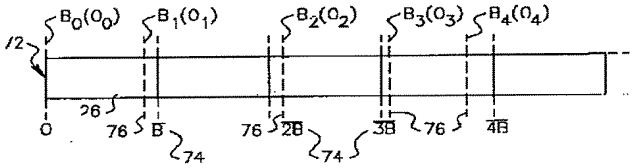
【図2】


キー #1c
50
キー #1b
キー #1a
フレーム1c-Cr
フレーム2c-Cr
フレーム3c-Cr
フレーム4c-Cr
フレーム1b-Cb
フレーム2b-Cb
フレーム3b-Cb
フレーム4b-Cb
フレーム1a-Y
フレーム2a-Y
フレーム3a-Y
フレーム4a-Y
54
26

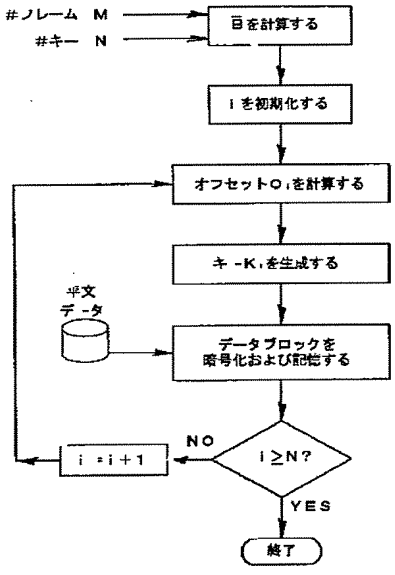
【図4】


フレーム17
フレーム18
フレーム19
フレーム20
フレーム21
フレーム22
フレーム23
フレーム24
26
ブロック #3
フレーム9
フレーム10
フレーム11
フレーム12
フレーム13
フレーム14
フレーム15
フレーム16
ブロック #2
54
26
フレーム1
フレーム2
フレーム3
フレーム4
フレーム5
フレーム6
フレーム7
フレーム8
ブロック #1

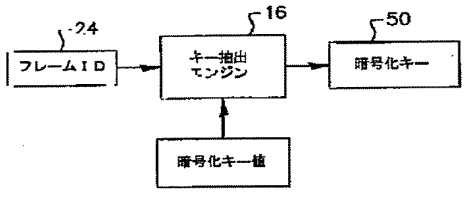
【図7】


$B_0(O_0)$
$B_1(O_1)$
$B_2(O_2)$
$B_3(O_3)$
$B_4(O_4)$
12
26
0
76
B
74
76
2B
74
3B
76
4B

【図8】


#ノーム M
#キー N
Bを計算する
iを初期化する
オフセットOiを計算する
キーKiを生成する
平文データ
データブロックを暗号化および記憶する
i=i+1
NO
i≧N?
YES
終了

【図9】


24
フレームID
16
キー抽出エンジン
50
暗号化キー
暗号化キー値